Product Guide

McAfee Threat Intelligence Exchange 1.0.0

For use with ePolicy Orchestrator 5.1.1 Software

COPYRIGHT
Copyright © 2014 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface **5**

About this guide 5

Audience 5

Conventions 5

Find product documentation 6

1 Overview **7**

Benefits of Threat Intelligence Exchange 7

Threat Intelligence Exchange components 8

Threat Intelligence Exchange module 8

Threat Intelligence Exchange server 9

Data Exchange Layer 9

How Threat Intelligence Exchange works 11

How a reputation is determined 11

2 Using Threat Intelligence Exchange **13**

Getting started with Threat Intelligence Exchange 13

Building file prevalence and observing 13

Monitoring and making adjustments 13

Submitting files for further analysis 14

Blocking or allowing files and certificates 15

Create a Threat Intelligence Exchange module policy 16

Changing default threat reputations 16

Change default threat reputations 16

Change the reputation of a file or certificate 17

Import reputations 18

Change reputations using the McAfee ePO Web API 19

Determine where a file ran in your environment 19

Monitoring events 20

Viewing recent events 20

View details about recent threats 21

Responding to events 22

Setting a system's health status 22

Managing Data Exchange Layer brokers 23

Data Exchange Layer components 23

Add or update brokers 23

Add brokers to a DMZ 23

3 Reporting **25**

Viewing reports 25

Access reports 25

Index **27**

Contents

Preface

This guide provides the information you need to work with your McAfee product.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

1 Go to the McAfee ServicePortal at http://support.mcafee.com and click **Knowledge Center**.

2 Enter a product name, select a version, then click **Search** to display a list of documents.

1 Overview

McAfee® Threat Intelligence Exchange provides context-aware adaptive security for your enterprise environment.

Contents

- *Benefits of Threat Intelligence Exchange*
- *Threat Intelligence Exchange components*
- *How Threat Intelligence Exchange works*
- *How a reputation is determined*

Benefits of Threat Intelligence Exchange

The challenge in today's network environment is the growing number of devices and systems and their inability to communicate security information with each other. These devices and systems include the cloud, consumer products, mobile products, and managed nodes. Until now, they have acted as silos and were not intelligently managed as a whole. Threat Intelligence Exchange is changing that. It quickly analyzes files and content from several sources in your environment and makes informed security decisions based on a file's reputation and your specific criteria.

Imagine knowing exactly which computers are compromised by a specific file, then acting immediately to prevent the threat from spreading, even to remote networks and systems. You can see the specific system where the threat was first detected, where it went from there, and stop it immediately.

Threat Intelligence Exchange provides a security ecosystem that allows instant communication between endpoints, systems, and devices in your environment. This communication is made possible with a new technology called the *Data Exchange Layer (DXL)* framework.

Threat Intelligence Exchange provides these benefits:

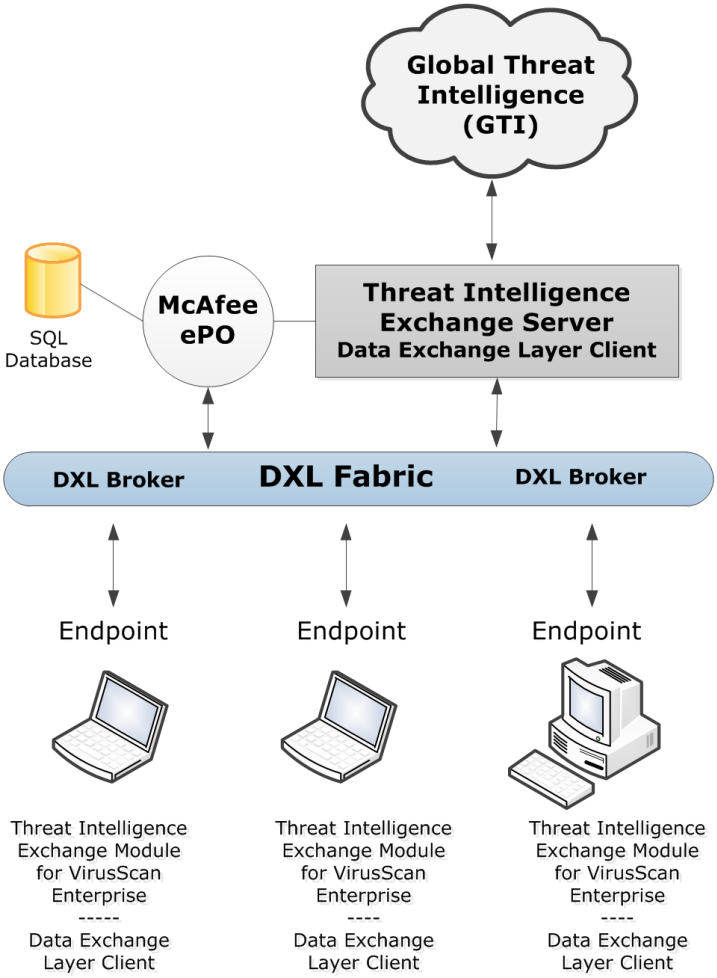
- Fast detection and protection against security threats and malware.
- The ability to know which systems or devices are compromised, and how the threat spread through your environment.
- The ability to immediately block or allow specific files and certificates based on their threat reputations and your risk criteria.
- Real-time integration with McAfee® Advanced Threat Defense and McAfee® Global Threat Intelligence™ (McAfee GTI) to provide detailed assessment and data on malware classification. This integration allows you to respond to threats and share the information throughout your environment.

Threat Intelligence Exchange components

Threat Intelligence Exchange includes multiple components.

- A module for McAfee® VirusScan® Enterprise
- A server
- The Data Exchange Layer client and brokers.

These components are installed as McAfee® ePolicy Orchestrator® (McAfee ePO™) extensions and add several new features and reports.



The module and server communicate file reputation information. The Data Exchange Layer framework immediately passes that information to managed endpoints. It also shares information with other McAfee products that access the Data Exchange Layer, such as McAfee® Enterprise Security Manager (McAfee ESM) and McAfee® Web Gateway.

Threat Intelligence Exchange module

The module for VirusScan Enterprise allows you to determine what happens when a file with a malicious or unknown reputation is detected in your environment. You can also view threat history information and the actions taken.

You can perform these tasks using the Threat Intelligence Exchange module.

- Create policies that allow or block files and certificates depending on their reputation. Or receive a prompt each time a file or certificate with a certain reputation attempts to run. You can also send files automatically to Advanced Threat Defense for further evaluation.
- View events on the Threat Intelligence Exchange dashboards. You can view cleaned, blocked, and allowed events for the past 30 days or by event type.

Threat Intelligence Exchange server

The server stores file and certificate reputation information. It passes that information to other systems and endpoints in your environment.

The server enables you to:

- Override a default file or certificate reputation to control what is allowed to run in your environment. For example, if your organization routinely uses a file that has an unknown security reputation, you can set its reputation to allow the file to run.
- Identify and track new files that attempt to run in your environment. If the new file is allowed to run, the server identifies which system or device was the first to run the file, and all other systems where the file was run.
- Instantly stop threats from spreading throughout your environment. Once the reputation of a file or certificate is detected as malicious (or suspicious, depending on your settings) it's immediately blocked from running anywhere in your environment.
- Identify which files were blocked and where they attempted to run. You can see where threats originate and see patterns as they occur. For example, specific systems might be more prone to detecting and blocking malicious files so you can increase the security settings on those systems.
- Specify the rules used in the policies, based on the types of systems. Rules are available for:
  - Systems that change frequently (programs and files are often installed and uninstalled)
  - Typical business systems that change infrequently
  - IT-managed systems that access critical or sensitive information and rarely change

Data Exchange Layer

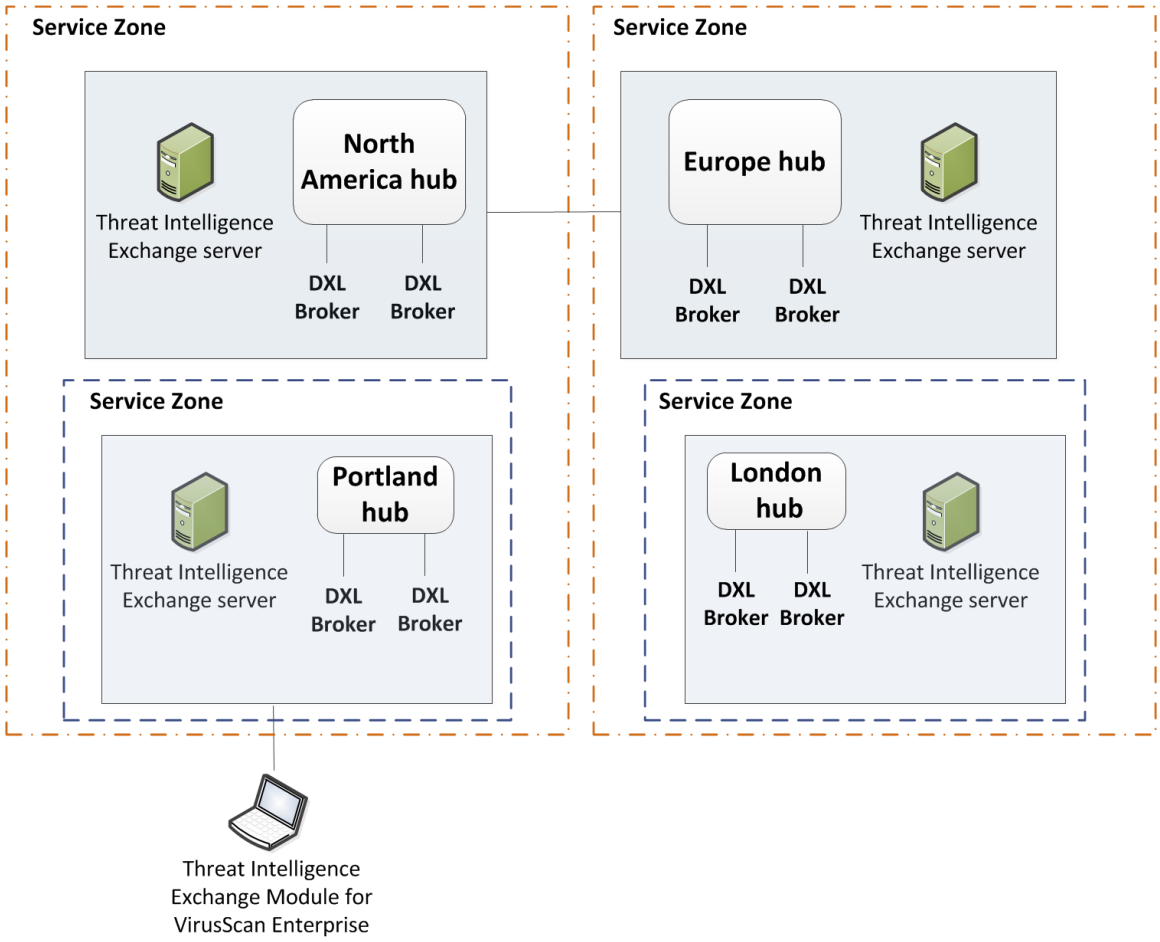
The Data Exchange Layer (DXL) includes client software and one or more brokers that allow bidirectional communication between endpoints on a network. The DXL client is installed on each managed endpoint, so threat information can be shared immediately with all other services and devices. This sharing of information reduces the spread of threats.

DXL works in the background, communicating with services, databases, endpoints, and applications. It receives and sends encrypted messages throughout your environment to track activity, risks, and threats in real time. Sharing reputation information as soon as it becomes available reduces the security assumptions that applications and services make about each other when they exchange information.

DXL clients maintain a persistent connection to their brokers regardless of their location. Even if a managed endpoint running the DXL client is behind a NAT (network address translation) boundary, it can receive updated threat information from its broker located outside the NAT.

DXL has these components:

- **Brokers** — Installed on managed systems and communicate messages between Threat Intelligence Exchange modules. The network of brokers tracks active consumers and dynamically adjusts the message routing as needed. Brokers can be organized into hubs.
- **Hubs** — Contain one or two brokers that are associated with a specific location. Hubs provide failover protection in a multi-broker environment. If a hub has two brokers, both act simultaneously. If one is unavailable, the other continues to function.
- **Consumers** — Modules, such as the Threat Intelligence Exchange module for VirusScan Enterprise, that receive and process messages from the brokers.
- **Service zones** — A service zone is associated with brokers and hubs and is used to route Threat Intelligence Exchange requests. In the following example, the highlighted boxes show the service zones defined. When the module sends a reputation request, it attempts to find a Threat Intelligence Exchange server in the Portland service zone first. If a server is not available in that zone, it looks in the North America service zone, because the Portland hub is part of the North America zone. Without specifying service zones, requests are sent in round-robin order and could be sent to the Europe or London hub first.
- **Data Exchange Layer client software** — Manages brokers, hubs, and service zones.



After installing the DXL brokers and client software, you create the hubs and zones for the brokers in your environment. This step is necessary only if you have several Threat Intelligence Exchange servers and DXL brokers.

How Threat Intelligence Exchange works

Threat Intelligence Exchange is the first product to use the Data Exchange Layer framework to share file and threat information instantly across the entire network environment.

In the past, you sent an unknown file or certificate to McAfee for analysis, then updated the file information throughout the network days later. Threat Intelligence Exchange enables file reputation to be controlled at a local level, your environment. You decide which files can run and which are blocked. The Data Exchange Layer shares the information immediately throughout your environment.

Scenarios for using Threat Intelligence Exchange

- **Immediately block a file** — Threat Intelligence Exchange alerts the network administrator of an unknown file in the environment. Instead of sending the file information to McAfee for analysis, the administrator can block the file. With the file prevented from running, the administrator can use Threat Intelligence Exchange to learn whether the file is a threat and how many systems ran the file.
- **Allow a custom file to run** — A company routinely uses a file whose default reputation is malicious, for example a custom file created for the company. Because this file is allowed, instead of sending the file information to McAfee and receiving an updated DAT file, the administrator can change the file's reputation to trusted and allow it to run without warnings or prompting.
- **Import known reputations** — A company has several files that are trusted and used regularly, and other files that are not allowed. Because the reputations are already known and set, the administrator can import that list of files and their reputations directly into the Threat Intelligence Exchange database and those reputations are used immediately with no further action.
- **Find additional information about a file** — Threat Intelligence Exchange notifies the network administrator of an unknown file. The administrator looks at the available reputation details for the file, then wants to learn more about it. The administrator can access VirusTotal from the Threat Intelligence Exchange module for VirusScan Enterprise to see more detailed information about the file.

How a reputation is determined

File and certificate reputation is determined when a file attempts to run on a managed system.

These steps occur when determining a file or certificate's reputation.

1. The end user or system attempts to run a file.
2. VirusScan Enterprise inspects the file and can't determine its validity and reputation.
3. The module for VirusScan Enterprise inspects the file and gathers file and local system properties of interest.
4. The module checks the local reputation cache for the file hash. If the file hash is found, the module gets the enterprise prevalence and reputation data for the file from the cache.
5. If the file hash is not found in the local reputation cache, the module then queries the Threat Intelligence Exchange server for the file hash. If the hash is found, the module gets the enterprise prevalence data (and any available reputations) for that file hash.

6 If the file hash is not found in the Threat Intelligence Exchange cache or database, the server queries McAfee GTI for the file hash reputation. If found, McAfee GTI sends the information back to the server.

   If Advanced Threat Defense is present and the file hash was not found in McAfee GTI, or if the policy on the endpoint indicates that the file should be sent to Advanced Threat Defense, the server sends the file for scanning. See the additional steps under *If Advanced Threat Defense is present*.

7 The server returns the file hash's enterprise age, prevalence data, and reputation to the module based on the data that was found. If this is the first time the file is seen in the environment, the server also sends a first instance flag to the module.

8 The module evaluates this metadata to determine the file's reputation:

- File and system properties
- Enterprise age and prevalence data
- Reputation

9 The module takes action based on the policy assigned to the system that is running the file.

10 The module updates the server with the reputation information and whether the file is allowed or blocked. It also sends threat events to McAfee ePO via the McAfee Agent.

11 The server publishes the reputation change event for the file hash.

If Advanced Threat Defense is present

If Advanced Threat Defense is present, the following process occurs.

1 If the system running the file has access to Advanced Threat Defense and this is the first time the file is seen in the environment, the Threat Intelligence Exchange server sends the file to Advanced Threat Defense for scanning.

2 Advanced Threat Defense scans the file and sends file reputation results to the Threat Intelligence Exchange server using the Data Exchange Layer. The server also sends the updated reputation information to all Threat Intelligence Exchange-enabled systems to immediately protect your environment.

2 Using Threat Intelligence Exchange

Contents

- *Getting started with Threat Intelligence Exchange*
- *Blocking or allowing files and certificates*
- *Changing default threat reputations*
- *Determine where a file ran in your environment*
- *Monitoring events*
- *Managing Data Exchange Layer brokers*

Getting started with Threat Intelligence Exchange

After you install Threat Intelligence Exchange, what do you do next?

The following examples provide an overview about how to use the Threat Intelligence Exchange module for VirusScan Enterprise and the Threat Intelligence Exchange server to detect and prevent threats in your environment. Detailed steps about using the module and server are in the following chapters.

Building file prevalence and observing

After installation and deployment, start building file prevalence and current threat information.

You can see what's running in your environment and add file and certificate reputation information to the Threat Intelligence Exchange database. This information also populates the graphs and dashboards available in the module where you view detailed reputation information about files and certificates.

To get started, create one or more Threat Intelligence Exchange policies to run on a few systems in your environment. The policies determine

- When a file or certificate with a specific reputation level is allowed to run on a system
- When a file or certificate is blocked
- When the user is prompted for what to do

While building file prevalence, you can run the policies in Observation mode. File and certificate reputations are added to the database but no action is taken. You can see what Threat Intelligence Exchange blocks or allows if the policy is enforced.

For details, see Create a Threat Intelligence Exchange module policy on page 16.

Monitoring and making adjustments

As the policies run in your environment, reputation data is added to the database.

Use the Event Manager and McAfee ePO Dashboards to see the files and certificates that are allowed or blocked based on the policies.

You can view detailed information in the Event Manager by system (computer), file, rule, or certificate and quickly see the number of items identified and the actions taken. Based on the information you see, you can adjust the reputation settings for specific files or certificates so that appropriate action is taken.

For example, if a file's default reputation is suspicious or unknown but you know it's a trusted file, you can change its reputation to trusted so that it runs in your environment without blocking or prompting. This is especially useful for internal or custom files used in your environment.

- Use the TIE Reputations feature to search for a specific file or certificate name. You can view details about the file or certificate, including the company name, SHA-1 Hash, description, and McAfee GTI information. For files, you can also access VirusTotal data directly from the TIE Reputations details page to see additional information.
- If you identified a harmful or suspicious file, you can quickly see which systems ran the file and might be compromised.
- Change a file or certificate's reputation as needed for your environment. The information is immediately updated in the database and sent to all devices in your environment. Files and certificates are blocked or allowed based on their reputation.

  If you're not sure what to do about a specific file or certificate, you can block it from running while you learn more about it. Unlike a VirusScan Enterprise Clean action, which might delete the file, blocking keeps the file in place but doesn't allow it to run. The file stays intact while you research it and decide what to do.
- Import file or certificate reputations into the database to allow or block specific files or certificates based on other reputation sources. This allows you to use those settings for specific files and certificates without having to set them individually on the server.

Submitting files for further analysis

If a file's reputation is unknown or uncertain, you can submit it to Advanced Threat Defense for further analysis.

Advanced Threat Defense detects zero-day malware and combines anti-virus signatures, reputation, and real-time emulation defenses. Files can be sent from Threat Intelligence Exchange to Advanced Threat Defense automatically based on their reputation level and file size.

Threat Intelligence Exchange also includes a Product Improvement Program where file information is sent directly to McAfee for analysis and to collect file reputation information. The following anonymous information is sent to McAfee and is used to further understand and enhance reputation information.

McAfee does not collect personally identifiable information, and does not share information outside of McAfee.

File and certificate information

- Threat Intelligence Exchange server and module versions
- Reputation override settings made with the Threat Intelligence Exchange server
- External reputation information, for example from Advanced Threat Defense

File-only information

- File name, path, size, product, publisher, and prevalence
- SHA and MD5 Hash information
- Operating system version of the reporting computer
- Maximum, minimum, and average reputation set for the file
- Whether the reporting module is in Observation mode
- Whether the file was allowed to run, was blocked, or cleaned
- The product that detected the file, for example Advanced Threat Defense or VirusScan Enterprise

Certificate-only information

- SHA Hash information
- The name of the certificate's issuer and its subject
- The date the certificate was valid, and its expiration date

Blocking or allowing files and certificates

Files and certificates have threat reputations based on content and properties. The Threat Intelligence Exchange policies determine whether files and certificates are blocked or allowed on systems in your environment based on reputation levels.

Three security levels are available depending on how you want to balance the rules for particular types of systems. Each level is associated with specific rules that identify malicious and suspicious files and certificates.

- **High change systems** — These are systems that change frequently, often installing and uninstalling programs and receiving frequent updates. Examples of these systems are computers used in development environments. Fewer rules are used with policies that use this setting and users see minimum blocking and prompting when new files are detected.
- **Typical systems** — These are typical business systems where new programs and changes are installed infrequently. More rules are used with policies that use this setting and users see more blocking and prompting.
- **Low change systems** — These are IT-managed systems with tight control and little change. Examples of these are systems that access critical or sensitive information in a financial or government environment. This setting is also used for servers. The maximum number of rules are used with policies that use this setting and users see even more blocking and prompting.

To view the specific rules associated with each security level, click **Menu** | **Server Settings**. In the Setting Categories list, click **Threat Intelligence Exchange module for VSE**.

When determining which security level to assign a policy, consider the type of system where the policy is used, and how much blocking and prompting you want the user to encounter. After you create a policy, assign it to one or more computers or devices to determine how much blocking and prompting occurs. After the policy runs in your environment for a time, you might need to edit some of the settings to fine-tune what is being allowed, blocked, and prompted.

Create a Threat Intelligence Exchange module policy

Policy settings determine when a file or certificate is allowed to run, is blocked, or if users are prompted what to do.

Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** list, click **Threat Intelligence Exchange module for VSE 1.0.0**.
3. Click **My Default**, then click **Duplicate** to create a policy.
4. Enter a name for the new policy and a brief description, then click **OK**.
5. Complete the fields on the Policy Catalog page.

Changing default threat reputations

Threat Intelligence Exchange has the ability to set file and certificate reputations for your specific environment.

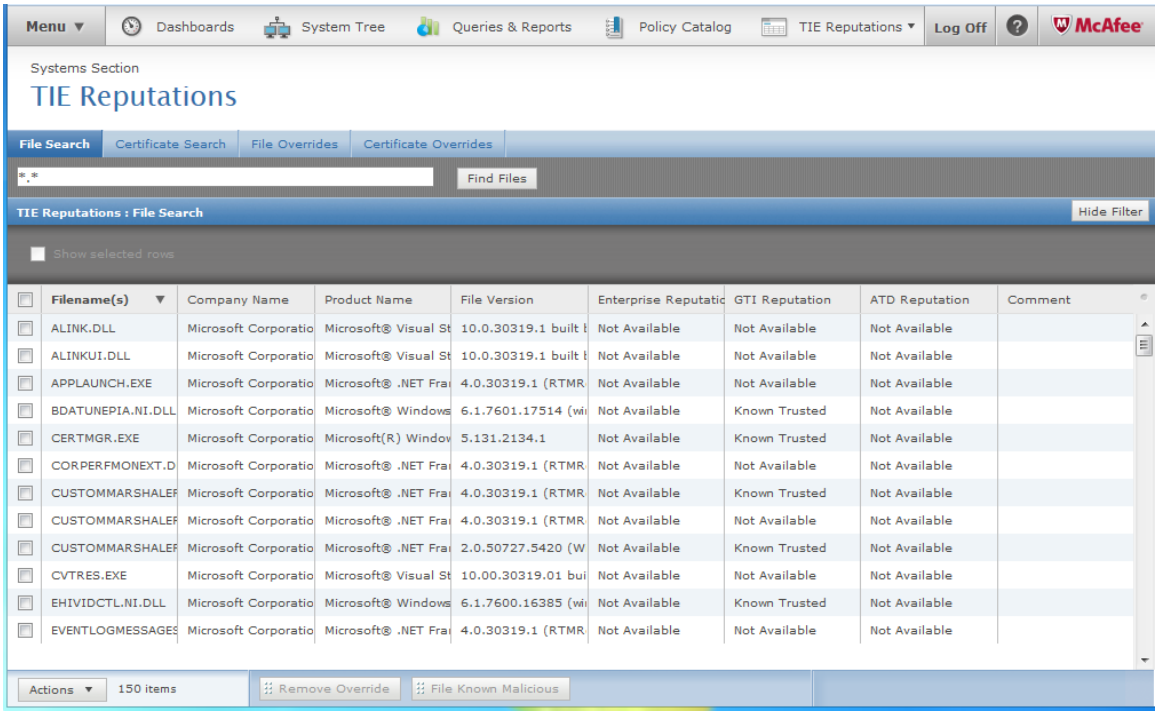
Change default threat reputations

You decide which files and certificates are allowed to run and which are blocked, rather than an external entity that sets default file reputations used by everyone. Each file and certificate has a known reputation setting, or risk, associated with it. That information is determined and then stored in the Threat Intelligence Exchange database.

Based on settings in the Threat Intelligence Exchange policies, files and certificates are allowed or blocked, or prompts the user according to their reputation. To fine-tune what is allowed or blocked in your environment, you can override default reputation settings for specific files and certificates .

File and certificate reputations are added to the Threat Intelligence Exchange database in three ways:

- Run the Threat Intelligence Exchange module for VirusScan Enterprise
- Advanced Threat Defense sends reputation information over the Data Exchange Layer framework and is added to the database
- Manually adds files or certificates to the database



Scenarios

- Your site commonly uses a file whose default reputation is unknown or might be classified malicious because it is a custom file. Because you know the file is safe, you can change its reputation to trusted so that it runs without interference.
- You want to block a common, trusted file from running in your environment, such as a file that allows remote desktop access. You can change its reputation to malicious, blocking it from running on systems in your environment.
- Users are notifying you that they are prompted when a specific file tries to run. You look up the file's reputation and see that is in unknown. You then look at the file details and determine that it is a trusted file. You can then change its reputation to trusted so that it no longer prompts users.
- You have set file or certificate reputations and you want to import them into the Threat Intelligence Exchange database. You can add those reputations one at a time, or in a batch using an XML file.

Change the reputation of a file or certificate

Change the reputation of a file or a certificate to allow or block it in your environment.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **TIE Reputations**.

2 Click the **File Search** or **Certificate Search** tab.

3 Search for files or certificates by name or by file type, such as .dll or .exe. You can also use wildcard search characters * or ?.

To view details about a specific file or certificate, including its hash number, click its name. Examine the details and VirusTotal information for the file to determine how to classify it.

4 Select items in the list and use the **Actions** menu to set reputation override settings. The files or certificates are then added to the overrides list.

   You can add a note about the change, for example, `Researched the file's reputation. Blocking this file.`

5 To verify the change, click the **File Overrides** or **Certificate Overrides** tab to see that the file or certificate is listed with its updated reputation.

Import reputations

Import existing file or certificate reputation information to the Threat Intelligence Exchange database.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **TIE Reputations**.

2 Click the **File Overrides** or **Certificate Overrides** tab.

3 From the **Actions** menu, click **Import Reputations**.

4 In the **Import Reputations** dialog box, specify whether to import an XML file with one or more reputations, or a single reputation.

- **Select the reputation XML file to import** — Browse to the file location. See the following topic about the XML import file requirements.
- **Import single reputation** — Enter the information for the file.

Requirements for importing an XML file

When importing reputation information in an XML file, the file must meet these requirements.

Specifying the reputation as a number

You must specify the file or certificate reputation as a numerical value in the XML file.

Reputation setting	Numerical value
Known trusted	99
Most likely trusted	85
Might be trusted	70
Unknown	50
Might be malicious	30
Most likely malicious	15
Known malicious	1
Not set	0

File reputations

For each file, include its SHA-1 Hash and MD5 numbers. The file name is optional, but including it helps identify it in reports.

Certificate reputations

For each certificate, include its SHA-1 Hash and Public Key SHA-1 numbers. The certificate name is optional, but including it helps identify it in reports.

Example import file

```
<?xml version="1.0" encoding="UTF-8"?>
<TIEReputations>
     <FileReputation>
                    <FileName>HackIt.exe</FileName>
                    <SHA1Hash>0x98AF3632E17677A8A23739F720B1A2F215CB8836</SHA1Hash>
                    <MD5Hash>0xDEF30CBEA881149C2AFFDF9A059FB751</MD5Hash>
                    <ReputationLevel>15</ReputationLevel>
     </FileReputation>
     <FileReputation>
                    <FileName>trayMan.dll</FileName>
                    <SHA1Hash>0x7F618396A910908019B5580B4DA9031AF4A433CA</SHA1Hash>
                    <MD5Hash>0xB2B3DAE040F6B5AE1DF52B0CD7631A18</MD5Hash>
                    <ReputationLevel>15</ReputationLevel>
                    <Comment>Comment for ALTTAB</Comment>
     </FileReputation>
     <FileReputation>
                    <FileName>cabinet.dll</FileName>
                    <SHA1Hash>0x98AF3632E17677A8A23739F720B1A2F215CB8837</SHA1Hash>
                    <MD5Hash>0xDEF30CBEA881149C2AFFDF9A059FB759</MD5Hash>
                    <ReputationLevel>15</ReputationLevel>
                    <Comment>Comment for cabinet.dll</Comment>
     </FileReputation>
     <FileReputation>
                    <SHA1Hash>0xD182CF4C0F7550064BAA3A825E86DE8DA1D3290B</SHA1Hash>
                    <MD5Hash>0x36060A75D9EDB1AEF0825988C7DD8511</MD5Hash>
                    <ReputationLevel>15</ReputationLevel>
                    <Comment>Comment for PORTABLEDEVICEAPI</Comment>
     </FileReputation>
     <FileReputation>
                    <SHA1Hash>0xCAC3CB1EFE7FD53A9AC2C8825DACCC22EDFDFED7</SHA1Hash>
                    <MD5Hash>0xC693E642ACFBDD76433AF6BE3C3EEE6F</MD5Hash>
                    <ReputationLevel>15</ReputationLevel>
                    <Comment>Comment for PORTABLEDEVICECONNECTAPI</Comment>
     </FileReputation>
</TIEReputations>
```

Change reputations using the McAfee ePO Web API

Use the McAfee ePO Web API to use scripts to change the default reputation for files and certificates.

Threat Intelligence Exchange includes the `tie.setReputations` command for use with the McAfee ePO Web API. Use the `core.help` command to see details about syntax and options used with the `tie.setReputations` command. Additional syntax includes:

```
tie.setReputations [fileReps] [certReps]
Json string for file and/or certificate reputation(s) with Base64 encoded hash
values.Atleast one of fileReps or certReps needs to be specified.Both can be
specified too.
Parameters:
fileReps (param 1) - Json string of file reputation(s). Ex
[{"sha1":"frATnSF1c5s8yw0REAZ4IL5qvSk=","md5":"8se7isyX+S6Yei1Ah9AhsQ==","reputation":"99"},
{"sha1":"d3HtjhR0Eb3qN6c+vVxeqVVe0t4=","md5":"V+0uApv5yjk4PSpnHvT7UA==","reputation":"99"}]
certReps (param 2) - Json string of certificate reputation(s). Ex
[{"sha1":"frATnSF1c5s8yw0REAZ4IL5qvSk=","publicKeySha1":"frATnSF1c5s8yw0REAZ4IL5qvSk=","reput
ation":"99"}]]
```

For details about using the Web API, see the *McAfee ePO Web Scripting Guide*.

Determine where a file ran in your environment

See which systems in your environment ran a particular file. You can see the system name and the date the file first ran on that system.

Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Systems** | **TIE Reputations**.
2. Click the **File Search** tab.
3. Enter a specific file name, or search for files by name or by file type, such as .dll or .exe. You can also use wildcard search characters * or ? when searching.
4. Select the file that you want to see.
5. From the **Actions** menu, click **Where Has File Run**.

Systems that have run the file are listed, including the system name, IP address, and the first date the file ran on that system.

Monitoring events

The TIE module for VSE Events page shows recent Threat Intelligence Exchange events and security threats, and the actions taken.

Viewing recent events

Viewing recent events allows you to see threat information about your systems.

You can view enforced or observed events:

- **Enforcement Events** — Events that occur as a result of an enforced Threat Intelligence Exchange policy.
- **Observation Events** — Events that occur if the policy is enforced. It allows you to view, evaluate, and adjust policy and configuration settings before enforcing them. You can see which files or certificates are causing events, and change their reputation settings so they no longer generate an event.

You can view threat events in several ways and drill down for more information:

Past 30 days — Event summary information for the past 30 days.

Top 10 — The top 10 events by system, file, or certificate.

Certificate — The certificate name, its SHA1 value, and the number of certificates that were cleaned, blocked, or prompted.

File Hash — The file name and SHA1 value, and the number of files that were cleaned, blocked, or prompted.

Rule — The rule name, events where the rule was applied, and the number of rules that were cleaned, blocked, or prompted.

System — The system name, total events for that system, and the number of events that were cleaned, blocked, or prompted on a particular system.

Examples

- If a specific system regularly prompts users, select the system from the list on the TIE module for VSE Events page. You can then see details about the specific files or certificates that are causing the prompts. Select individual files or certificates from the Events page and change their reputation levels to allow or block them so that they no longer generate a prompt.
- If a specific file generates events, select it from the list on the Events page and see on which systems tried to run it and what action was taken. You can then change the file's reputation so that it no longer generates events. For example, if the file generates a prompt and you want it blocked, change its reputation so that it is blocked and does not generate an event.

View details about recent threats

View information about recent files and certificates seen in your environment and the actions taken.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Reporting** | **TIE module for VSE Events**.

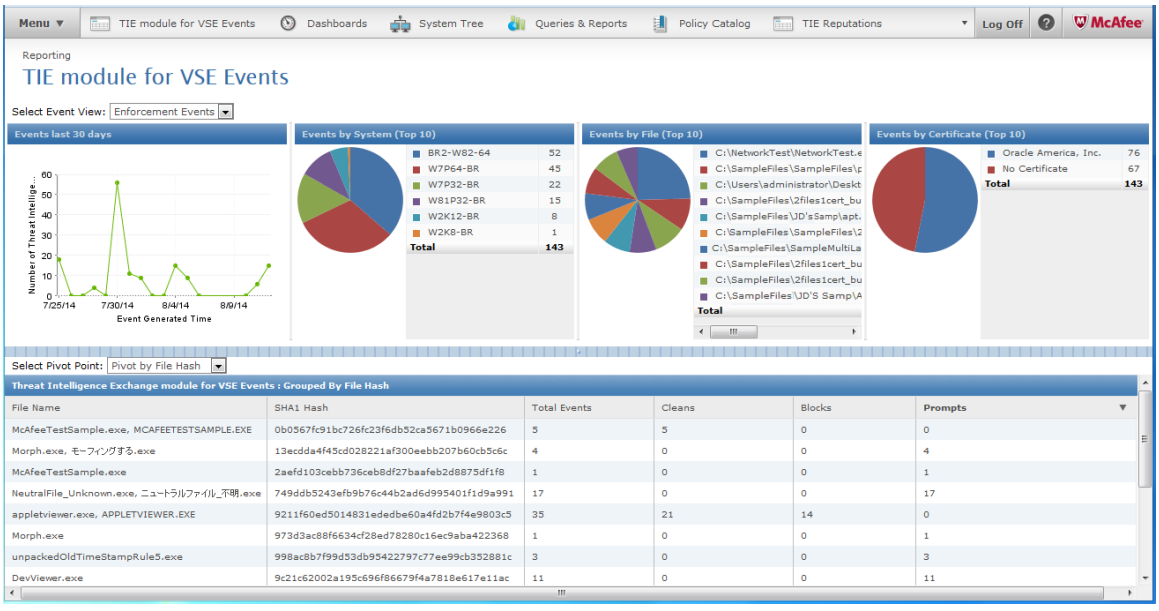
The **TIE module for VSE Events** page shows several views of recent events.

2 In the **Select Event View** drop-down list, select the type of events to show.

- **Enforcement Events** show enforced policy events and the actions taken.
- **Observation Events** show the observed policy events with no action taken.

3 Select a chart to see detailed information.

4 In the **Select Pivot Point** drop-down list, select how to view events: by certificate, file hash, rule, or system. Then, select a specific item in the list to see more details.



Responding to events

Use the information on the **TIE module for VSE Events** page to adjust file and certificate reputations to prevent threats and other events.

When you drill down into recent events on the **Events** page, you can see the items that are generating events. If you see a file or certificate that's causing a block or prompt based on its reputation, you can change its reputation setting to stop the event. Select the file to see its details, then use the options on the Actions menu to change its reputation.

Setting a system's health status

Based on the threat events reported and files executed on a system, you can set it's health status to see compromised systems and healthy systems.

As events are reported and files are blocked or allowed, you can set the health status of specific systems. You can then monitor compromised systems for threat events, or change policy settings for systems that have run, or often block, malicious or suspicious files.

There are three system health settings: **Compromised**, **Healthy**, and **Possibly Compromised**. You can manually set the health status for particular systems using Threat Intelligence Exchange, or create an Automatic Response query or Server Task in McAfee ePO to apply a status automatically. You can then create a query that looks for compromised systems and run a server task to take a specific action on those systems.

When creating the Automatic Response in McAfee ePO, the system health status options on are the Actions page of the wizard. Choose the **Run System Command** action, and from the **System command** drop-down, choose **Set System Health Indicator** and specify the health status.

For details about creating Automatic Responses, queries, and server tasks, see the *McAfee ePolicy Orchestrator Best Practices Guide*.

Set system health status

Manually set the Threat Intelligence Exchange health status for systems to indicate if it's healthy, compromised, or potentially compromised.

Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Systems Section** | **System Tree**.
2. Select one or multiple systems.
3. From the **Actions** menu, click **System Health**, then choose the health status to apply to the selected systems.

The health status is displayed in the TIE System Health column on the System Tree.

To display the TIE System Health column on the System Tree, from the **Actions** menu, click **Choose Columns**, then from the **Available Columns** list, select **TIE System Health**.

Managing Data Exchange Layer brokers

The Data Exchange Layer (DXL) includes a client and at least one broker that allows bidirectional communication between endpoints on a network.

Data Exchange Layer components

The Data Exchange Layer framework has these components.

Brokers — Installed on managed systems and communicate messages between Threat Intelligence Exchange modules. The network of brokers tracks active consumers (such as the Threat Intelligence Exchange module for VirusScan Enterprise) and dynamically adjusts the message routing as needed. Brokers can be organized into hubs.

Hubs — Contain one or two brokers that are associated with a specific location. Hubs provide failover protection in a multi-broker environment. If a hub has two brokers, both act simultaneously; if one is unavailable, the other continues to function. You can create as many hubs as needed, but a broker can be assigned to only one hub.

Service zones — A service zone is associated with brokers and hubs and is used to route Threat Intelligence Exchange requests. When the module for VirusScan Enterprise sends a reputation request, it goes to the local service zone first. If the request can't be serviced there, it then goes to the next service zone in the hierarchy.

Data Exchange Layer client software — Manages brokers, hubs, and service zones.

As Threat Intelligence Exchange runs in your environment, you might want to add new Data Exchange Layer brokers or reorganize existing brokers into new hubs and service zones. You can also install brokers in a demilitarized zone (DMZ) so that remote workers can access the latest threat information.

Add or update brokers

As Threat Intelligence Exchange runs in your environment, you can fine-tune your broker hierarchy to accommodate changes to your environment.

You might want to install more Threat Intelligence Exchange servers and brokers throughout your environment as you add new endpoints and systems.

Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Configuration** | **Server Settings** | **DXL Topology**.
2. On the DXL Topology page, click **Edit** to create hubs and assign brokers. Brokers not assigned to a hub are listed below the hubs.
3. Select an item from the **Actions** menu to create or delete a hub, or to detach a broker from its current hub.

Add brokers to a DMZ

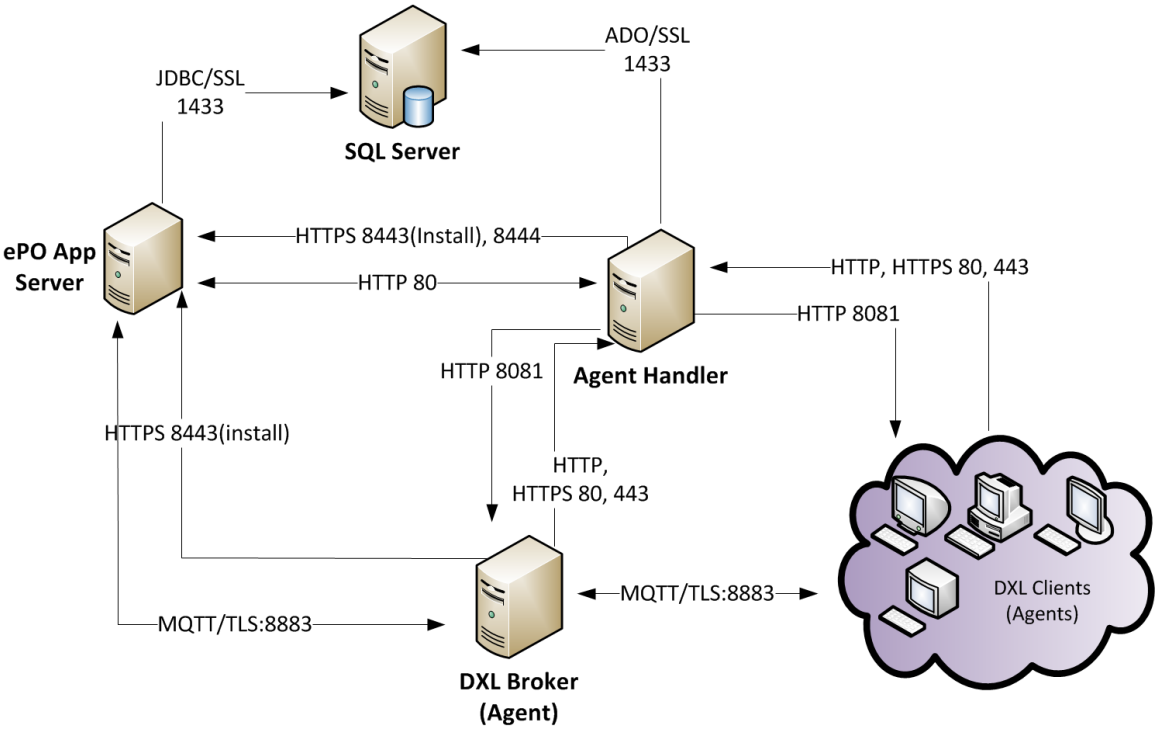
You can install Data Exchange Layer brokers in a demilitarized zone (DMZ) where publicly accessible servers are not allowed.

Installing a broker in the DMZ allows remote users to access information from products that use the Data Exchange Layer, such as Threat Intelligence Exchange.

You must have an Agent Handler in the DMZ and your network must be configured to support this. McAfee ePO communicates with the Data Exchange Layer broker to share configuration, policy, and performance information via the Agent on the broker.

To use a Data Exchange Layer broker in a DMZ, firewall rules are necessary. Also, the Data Exchange Layer topology must be structured in a way that allows communication from brokers in the DMZ to brokers in the internal network. The DXL Topology page enables you to create this structure. To access the DXL Topology page, click **Menu** | **Configuration** | **Server Settings** | **DXL Topology**.

This diagram shows the default ports used.



3 Reporting

You can access Threat Intelligence Exchange reports from the McAfee ePO Queries & Reports feature. There are reports for the Threat Intelligence Exchange server, the module for VirusScan Enterprise, and the Data Exchange Layer client.

Viewing reports

Threat Intelligence Exchange includes several reports that show threat information for files, certificates, and events.

The reports are available in the McAfee ePO **Queries & Reports** feature. They show the following information:

- New files and certificates seen in the enterprise
- Files and certificates organized by reputation
- Files and certificates with changed reputations
- Top 10 systems with new files or certificates
- Blocked, allowed, and cleaned events
- Observed events

Access reports

You create and view Threat Intelligence Exchange reports using McAfee ePO.

Task

For option definitions, click **?** in the interface.

1. In McAfee ePO, click **Menu** | **Reporting** | **Queries & Reports**.
2. To quickly find Threat Intelligence Exchange reports, use the **Quick find** box.
   - For server reports, enter `TIE`
   - For module reports, enter `module for VSE`
   - For Data Exchange Layer reports, enter `DXL`.
3. Click **Run** to see the report data.

See the McAfee ePO documentation for details about creating and using queries and reports.

Index

A

about this guide 5
Advanced Threat Defense 14
    configuring for TIE 16
    sending files to 15
    used in determining reputations 11
allowing files and certificates 15

B

blocking files and certificates 15
brokers for Data Exchange Layer 9, 23
    updating 23

C

certificates
    blocking or allowing 16
    changing a reputation 16
    how reputations are determined 11
    importing a reputation 18
compromised systems 22
conventions and icons used in this guide 5

D

Data Exchange Layer
    about 9
    adding and updating brokers 23
    adding brokers to a DMZ 23
    brokers 9
    creating hubs 23
    creating service zones 23
    hubs 9
    managing brokers 23
    service zones 9
determine
    what is blocked or allowed 16
    where a file has run 19
DMZ
    adding Data Exchange Layer brokers 23
documentation
    audience for this guide 5
    product-specific, finding 6
    typographical conventions and icons 5

E

enforced events 20
events
    enforced 20
    observed 20
    setting system health status 22

F

files
    blocking or allowing 16
    changing a reputation 16
    determine where a file has run 19
    how reputations are determined 11
    importing a reputation 18

G

getting started with Threat Intelligence Exchange 13
Global Threat Intelligence 16

H

hubs for Data Exchange Layer 9
    creating 23

I

importing file and certificate reputations 18
    import file requirements 18

M

marking a system as compromised 22
McAfee ePO Web API 19
McAfee ServicePortal, accessing 6
module for VirusScan Enterprise
    creating policies 16

O

observed events 20
offline behavior 16

P

policies
    creating 16

Product Improvement Program 14
prompting
    setting up 16

R

reputations
    changing for a file or certificate 16
    changing using McAfee ePO API 19
    how they are added to the database 16
    how they are determined 11
    import file requirements 18
    importing into the database 18

S

security levels
    examples 15
server
    about 9
service zones for Data Exchange Layer 9
ServicePortal, finding product documentation 6
submit files for further analysis
    Advanced Threat Defense 14
    Product Improvement Program 14
system health 22

T

technical support, finding product information 6
Threat Intelligence Exchange
    about 7
    benefits of 7
    creating policies 16
    Data Exchange Layer 9
    events 20
    module for VirusScan Enterprise 8
    server 9
    workflow examples 13

V

VirusScan clean action 16

W

where has a file run 19
workflow examples 13
    build file prevalence and observe 13
    monitor and make adjustments 13
    submit files for further analysis 14

McAfee
An Intel Company